

# Scambaiter: Understanding Targeted Nigerian Scams on Craigslist

Youngsam Park<sup>1</sup>, Jackie Jones<sup>2</sup>, Damon McCoy<sup>2</sup>, Elaine Shi<sup>1</sup> and Markus Jakobsson<sup>3</sup>

University of Maryland<sup>1</sup> George Mason University<sup>2</sup> ZapFraud<sup>3</sup>

# Nigerian scam is so prevalent!

## AusCERT 2013: Nigerian scam victim tells her story

**Summary:** Nigerian scam victim Jill explains how she was conned out of \$300,000 over a four year period.

Woman out \$400K to 'Nigerian scam' con artists

~~Suckers~~ Victims lost \$9.3 billion to 419 scammers in 2009

It's hard to believe that people are still falling for advance-fee fraud ...

# Targeted Nigerian scam variants

- Fake payment
  - “I sent a check (money order) with packaging fee. Please send your iPhone to my place ASAP!”
- Rental scam
  - “I’m out of country right now, so please send the rent and deposit via mail. Then I will send out the key!”
- Dating scam
  - “I’d love to meet you! Could you please help me buy a ticket to your state?”

# Our research...

- What's the target?
  - Targeted Nigerian scam with **fake PayPal payment** on **Craigslist**
- What have we done?
  - **Bait** scammers
  - **Automated conversation** with scammers
  - **Analyze** the large-scale scam data
- What can we learn?
  - Understand **how scammers work**
  - Look for the way to **deter the scams**

# Methodology

---

- Magnetic honeypot advertisements
  - Automated scam collection system
  - Scammers' IP collection
-

# Magnetic honeypot advertisements

- Sell **over-priced** items
- **Attract** scammers but **repel** legitimate users

[CL](#) > [boston](#) > [boston/camb/brook](#) > [all for sale / wanted](#) > [cell phones - by owner](#)

Reply to: see below      flag [?]: [mislabeled](#) [prohibited](#) [spam](#) [best of](#)      Posted: 2013-05-30, 6:25AM EDT

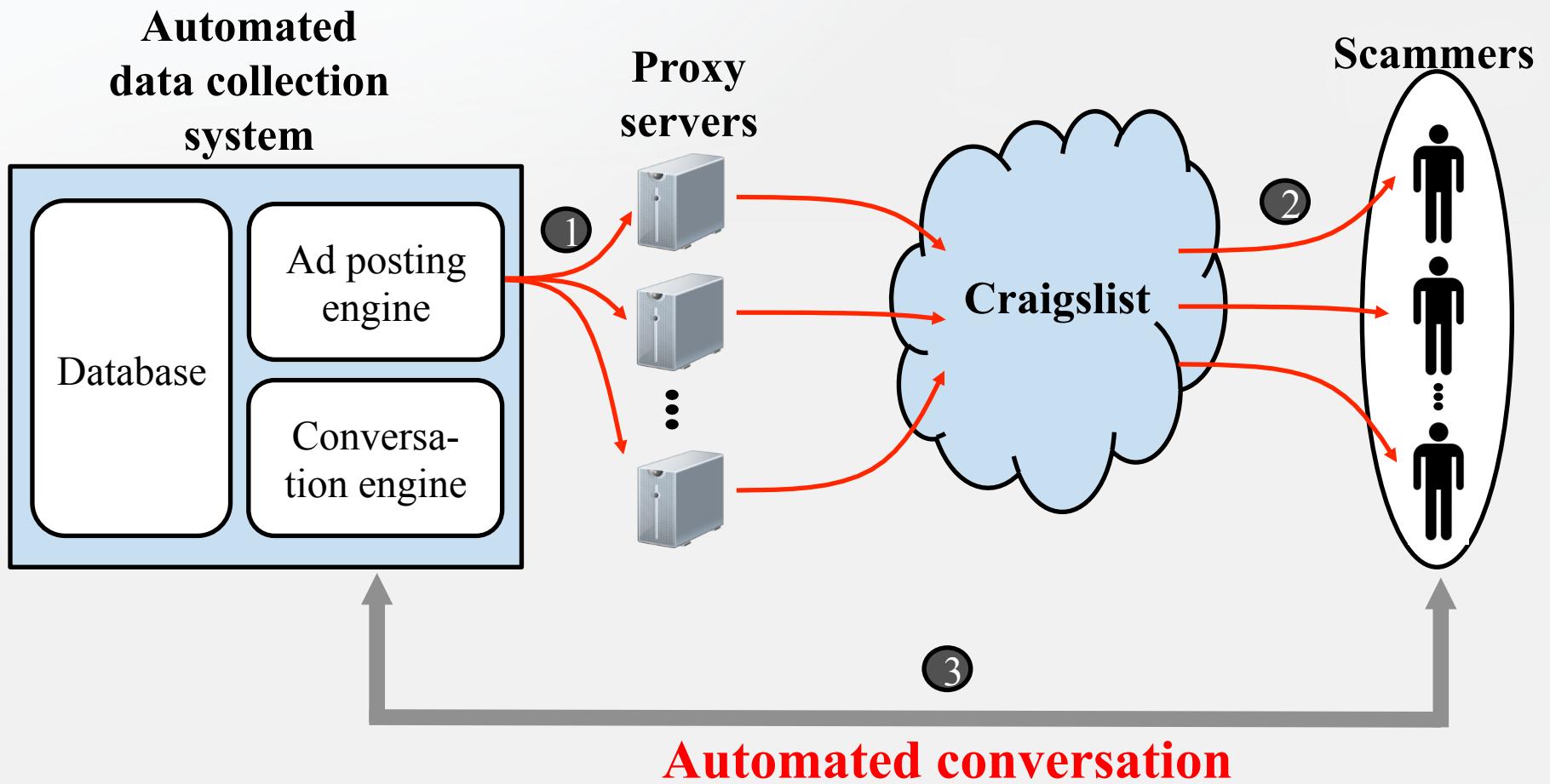
★ Samsung Galaxy Note II GT-N7100. - \$650



Samsung Galaxy Note II GT-N7100 - factory unlocked- 16GB Gray.  
5.55" high-resolution display.  
Draw and write straight onto the screen with your finger or included S Pen.  
16GB memory  
like new, in great condition.  
Asking for \$650.  
Please email me if interested.

Email: northruptony77@gmail.com  
\* Please put the subject of this ad in your email subject.

# Automated scam collection system



# Automated email conversation

Scammer's  
first response

Chloe Morgan <[@gmail.com](mailto:)> Jun 3 (11 days ago) ☆  
to me ▾  
..whats your last price and hope in mint condition? hear from you asap as its urgent

Scammer's  
second response

Chloe Morgan Jun 11 (3 days ago) ☆  
to me ▾  
Hi....Regarding the laptop i am buying from you hope you still have it for sale? Please  
get back to me ASAP as i am really interested buying

Scammer's  
third response

Chloe Morgan Jun 11 (3 days ago) ☆  
to me ▾  
Yea i was sending to Virginia...You got a PayPal Account??

Our first  
reply

Our second  
reply

Our third  
reply

@gmail.com Jun 11 (3 days ago) ☆  
to Chloe ▾  
Yes, it's still on sale.Please let me know if you need more information.

@gmail.com Jun 11 (3 days ago) ☆  
to Chloe ▾  
Sounds great. My paypal account is [junhyosung02@gmail.com](mailto:junhyosung02@gmail.com).  
Please let me know when the payment is done!!

# Fake payment notification

\*\*\*Notification Of An Instant Payment Made For Your Item ( Goods ) Using PayPal\*\*\*

Inbox Jun 11 (3 day)

service@int'l.paypal <postage\_fund@in.com>

Amount: \$420.00 USD  
Shipping and handling: \$0.00  
Postal Compensation: \$0.00  
Total Amount: \$420.00 USD

## service@int'l.paypal <postage\_fund@in.com>

Shop Without Sharing  
Your Financial Information  
PayPal. Privacy is built in.  
Learn more

GET UP TO 20% OFF TOP BRANDS.

You've got new funds!

craigslist

Dear Merchant

This email confirm that Mrs. Morgan Chloe, just sent you \$420.00 USD for a classified Market place item with PayPal.  
Mrs. Morgan Chloe is a Verified buyer .

### Payment Details

Amount: \$420.00 USD  
Shipping and handling: \$0.00  
Postal Compensation: \$0.00  
Total Amount: \$420.00 USD

### Item Information

Description: Goods  
Total Amount: \$420.00 USD

\*\*\*Please Note\*\*\*  
The buyer of this item has requested this item to be shipped to the below address.  
Buyer's Shipping Information.

Delivery Information:  
Name: Elizabeth Anne Erwin  
Shipping Address: 3129 Honeywood Lane apt c, Roanoke Va 24018

# IP address collection

- Embed product images in reply emails
- Limitation
  - **Only small part of scammers** may access the embedded images

junhyosung02@gmail.com

to Chloe ▾

Hi,

The price is 320, firm.

The condition is almost perfect since it was not used frequently.

Please let me know if you need more information.



Hi,

The price is 320, firm.

The condition is almost perfect since it was not used frequently.  
Please let me know if you need more information.

```
-----=2109632781039935239==  
Content-Type: text/html; charset="us-ascii"  
MIME-Version: 1.0  
Content-Transfer-Encoding: 7bit
```

```
<html><body>  
</body></html>
```

# Experimental results

---

- Scammer group classification
  - Scammer geolocation
  - Level of scam process automation
-

# Dataset overview

<b>Overview</b>	Experiment duration	<b>3 months</b>
	Cities/areas	<b>20</b>
	Product category	<b>4</b>
<b>Magnetic honeypot ads</b>	Total number of ads	<b>1,376</b>
<b>Emails</b>	First scammer responses received	<b>13,215 (9.6 per ad)</b>
	Fake PayPal payment emails	<b>751</b>

# Scammer group classification

- Conservative classification
  - Same email address, shipping address or phone number
  - Email addresses with 90% identical prefix

biglanre1@gmail.com  
biglanre10@gmail.com  
biglanre11@gmail.com  
biglanre12@gmail.com  
biglanre13@gmail.com  
biglanre14@gmail.com

- Result
  - Total number of groups: 1,234
  - Top 10 groups: 48%

# Scammer group classification

---

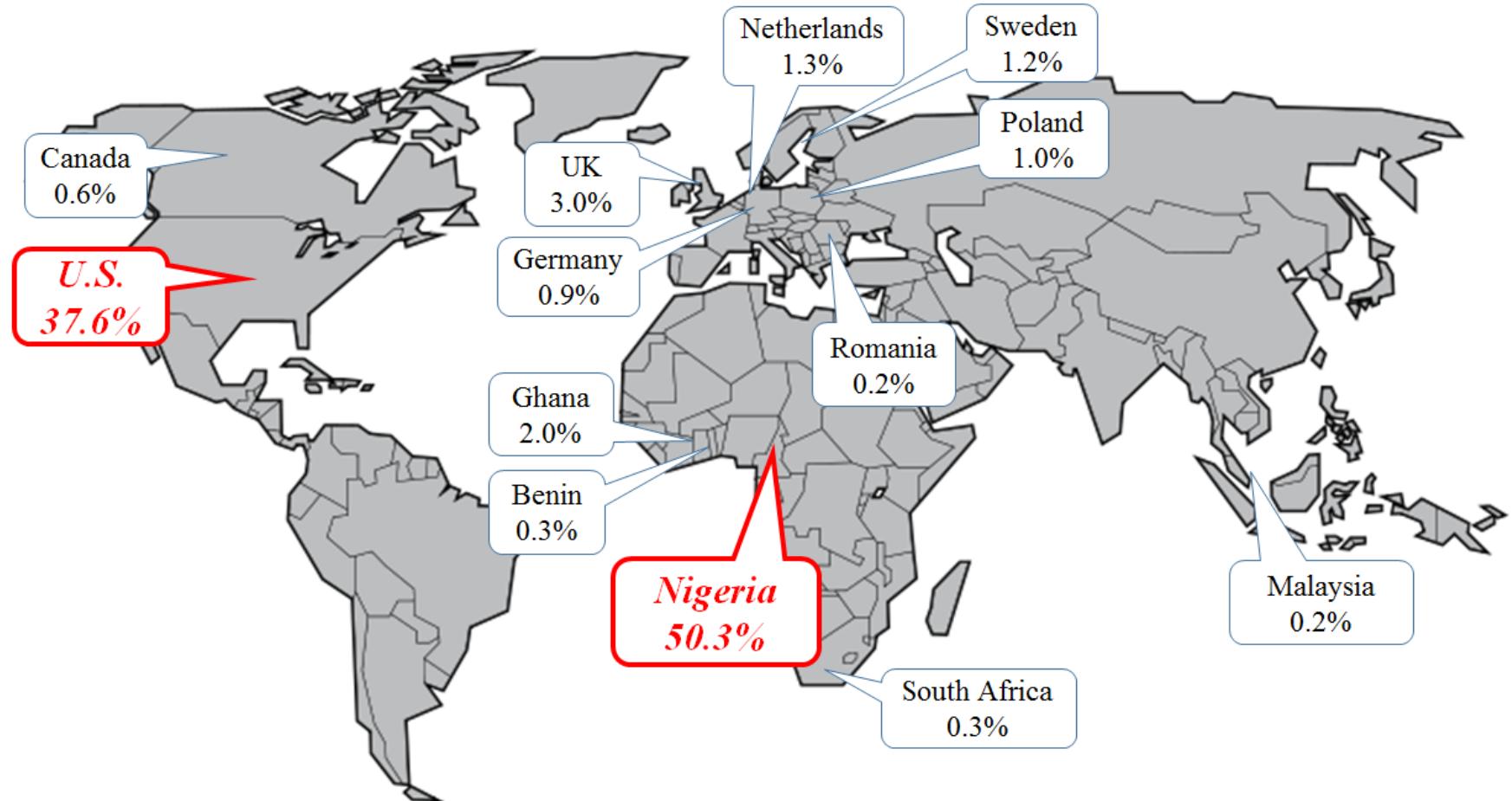
- Aggressive classification
  - Conservative classification
  - IP addresses belong to a same **class C subnet**
- Result
  - Total number of groups: **1,172**
  - **Top 10 groups: 56.8%**

# Scammer group classification

Group	# threads	# source addresses	# reply-to addresses	% source != reply-to	# cities	# product category
1	1096	178	23	100%	18	4
2	993	270	64	98.7%	20	4
3	885	313	48	95.8%	19	4
4	714	106	37	97.6%	20	4
5	700	52	11	98.6%	20	4
6	449	182	30	98.0%	17	4
7	441	60	17	97.5%	20	4
8	416	103	10	100%	20	4
9	330	19	8	94.8%	19	4
10	306	71	23	86.9%	20	4

Top 10 groups summary

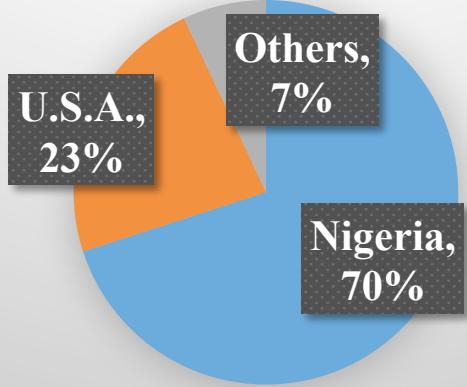
# Scammer IP address analysis



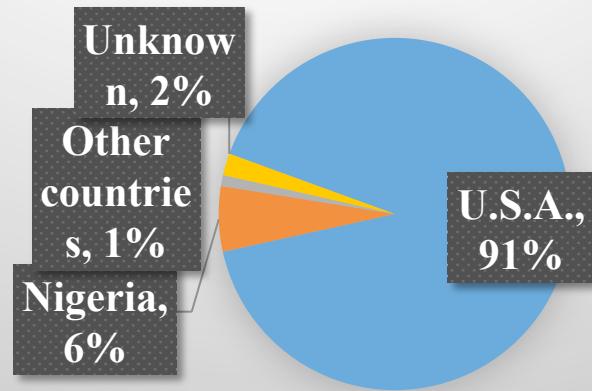
**Total number of IP addresses: 965**

# Shipping address/Phone number analysis

**Shipping address**



**Phone number**



# Level of automation

- Signs of automation
  - **Broken scripts** in email subject and content
  - **Duplicate/template** email contents
  - **Burst** of duplicate emails

## Broken Subject & Body

**[Subject:]** <span class=i h data-id=0:00x0x\_6FPl-zGRnuHX> </span>

**[Body:]** Is your <span class="i h" data-id="0:00x0x\_6FPlzGRnuHX"></span> still available for sale??  
i will reply right away. Thanks  
Sent from Devon's iPhone

**[Subject:]** <span class=i h data-id=3Fa3Le3I45Nd5I-c5Gcd624761cea879bf1558.jpg></span>

**[Body:]** <html><head><META http-equiv="Content-Type" content="text/html; charset=utf-8"></head><body>still for sale?; feel free to email me at darrenamos69@gmail.com</body></html>

# Level of automation

- Signs of manual labor
  - Curse/threat emails
  - Scam emails **peak during work hours of Nigeria**
  - Wrong email address/name

## Belligerence/Threats

- [words omitted] Please respond to this mail before the penalty decision is taken against you.

You are warned We are waiting for your mail before we can credit your account and this is due to the large increase in the rate of the online scams recorded in the previous years. [words omitted]

- [words omitted] i think if i did not hear back from you within next 24hrs i will have to contact FBI about your actions on Craigslist.org [words omitted]

- [words omitted] i will report you to paypal an FBI i give you 12h to get it ship [words omitted]

- Hey man what is going on i getting the FBI involve in this; is getting irritating [words omitted]

# Level of automation

---

- Conclusion
  - Scam process is **partially automated**
  - Scammers may need to **manually run automated tools**

# Summary

- Automated scam collection system
  - Magnetic honeypot ad posting
  - Automated email conversation
- Findings
  - A few large organizations
    - Top 10 groups: 48% of all collected scam trials
  - Geolocation of scammers
    - 90% from Nigeria and the United States
  - Methods and tools of scammers
    - Partially automated

# Future work

---

- Extending to other scam areas
  - Rental, dating scams
  - Fake payment scams on Ebay
- Filtering messages
  - Recurring themes, belligerent tones
  - Common linguistic features
- More precise tracking of scammer geolocation
  - GPS tracking

# Thank you!

[yspark@cs.umd.edu](mailto:yspark@cs.umd.edu)

# Appendix

- Recurring theme

- Present for family member and buyer overseas

- i want you to know you are also in safe hands and i want you to assure me that I won't be disappointed with it **cos am getting it for my cousin** the issue is that am not around i would have come and see it

- **i wanted to buy this for my Cousin; but the issue is am currently out of state** on a Contract Project .The contract is strictly no call due to the lack of reception in the area.

- **im arranging it for my cousing birthday who live in OKLAHOMA USA.** im off shore and Right now the only way i can make the payment is via paypal as i don't have access to my bank account online and theres no way i can issue out a check or something here

# Appendix

- Recurring theme
  - Present for family member and buyer overseas

Military member unable to come view product

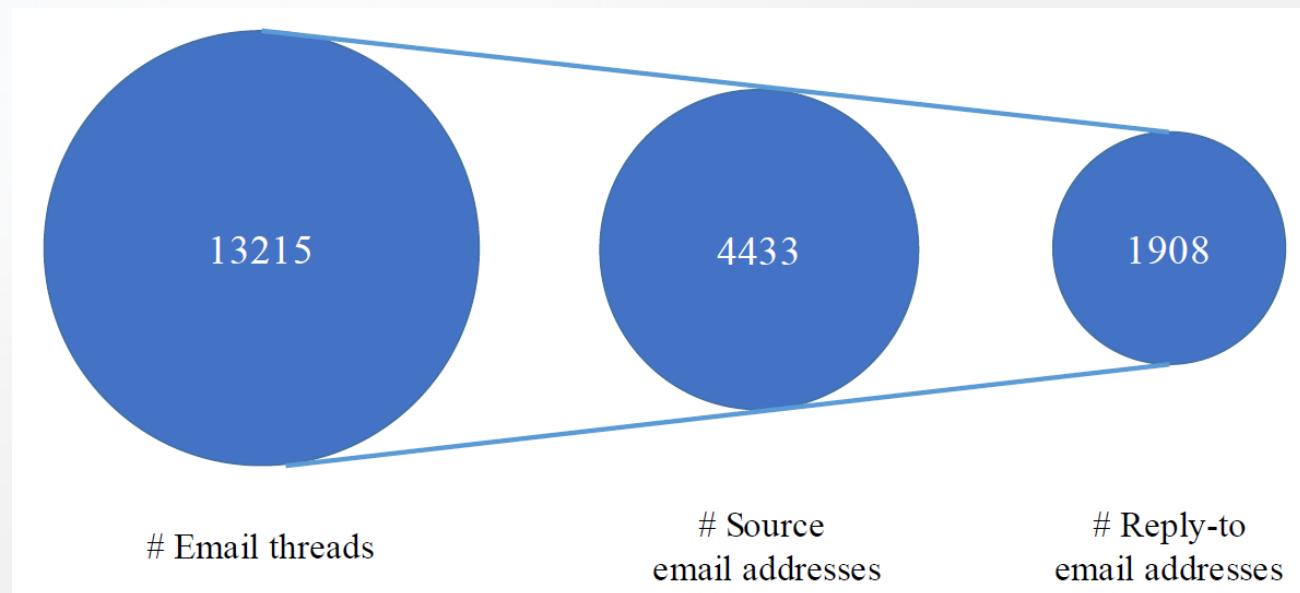
- because that is the only convenient means for me and due to my work frame i can not be able to get there and I promise everything will go smoothly.I really wish to be there to check out the item but **i don't have chance cause am very busy person (US MARINE)**. And am already back to camp but i will get home very soon
- i have no problem with the amount as **am a US marine** i work for the United State Marine Corps (USMC) but am currently hospitalized so **am on a treatment in New york**
- Am willing to buy and am a serious buyer but am **not around now so i won't be able to come to have a look because am in camp now I'm a Marine(US MARINE).**

# Appendix

- Recurring theme
  - Belligerence/Threats

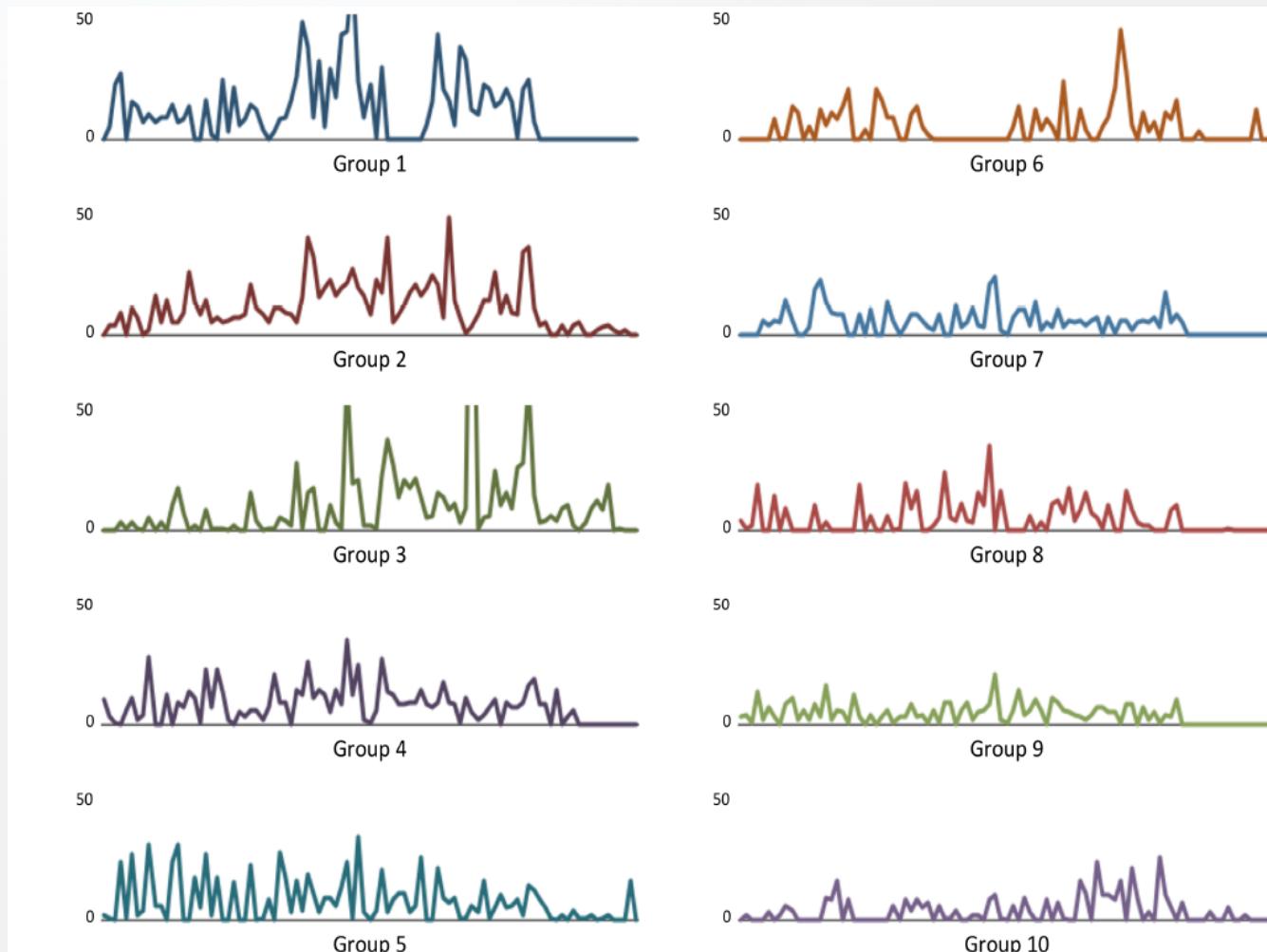
- Please respond to this mail before the penalty decision is taken against you. **You are warned.** We are waiting for your mail before we can credit your account and this is due to the large increase in the rate of the online scams recorded in the previous years.
- i think if i did not hear back from you within next 24hrs i will have to **contact FBI** about your actions on Craigslist.org
- **i will report you to paypal an FBI** i give you 12h to get it ship
- Hey man what is going on **i getting the FBI involve in this**; is getting irritating

# Scammer email accounts analysis



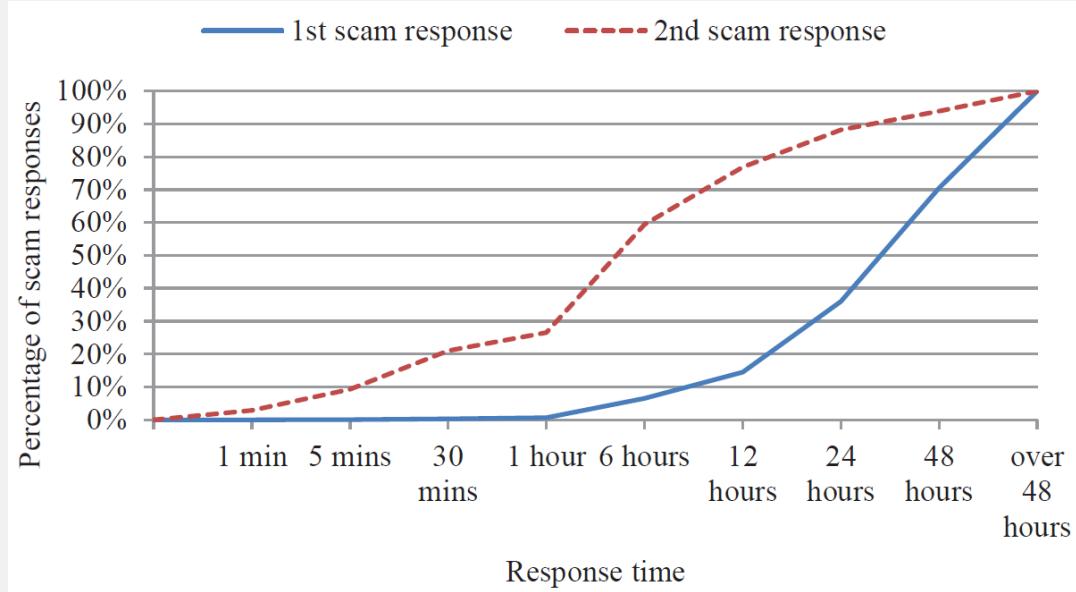
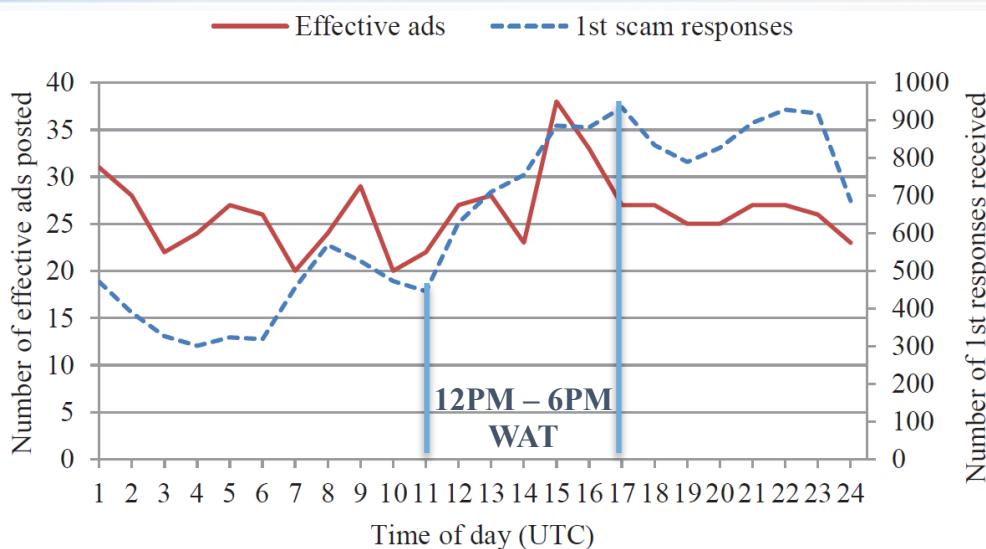
<b>First responses</b>	<b>13,125</b>
First responses with different source and reply-to addresses	10,826 (81.9%)
<b>Second responses</b>	<b>1,626</b>
Second responses with different source and reply-to addresses	316 (19.4%)

# Scammer group classification



Emails per day – top 10 groups

# Scammer pattern analysis



# Scammer IP address analysis

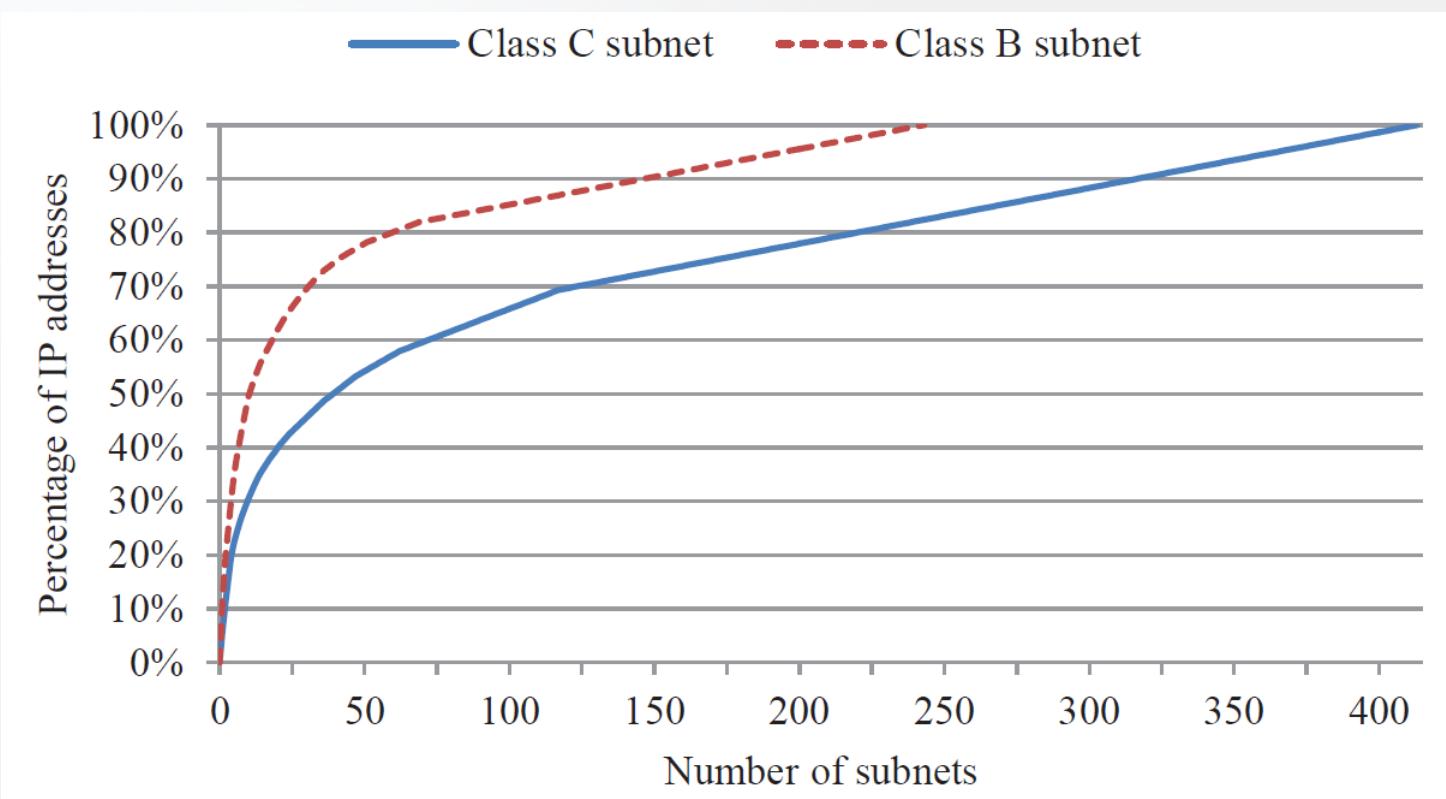
IP address	Percentage
Not in black/ graylist	43.9%
Blacklisted	40.4%
Graylisted	14.0%
Web crawler	1.7%

IP addresses blacklisted by  
*Project Honey Pot*

IP address	Country	# times observed	Blacklisted?
41.211.193.X	Nigeria	298	-
41.203.67.X	Nigeria	241	Yes
41.203.67.X	Nigeria	204	Yes
41.203.67.X	Nigeria	160	Yes
41.211.198.X	Nigeria	93	-
41.206.15.X	Nigeria	89	Yes
41.184.21.X	Nigeria	89	Graylisted
41.206.15.X	Nigeria	88	Yes
41.211.201.X	Nigeria	85	-
41.206.15.X	Nigeria	79	Yes

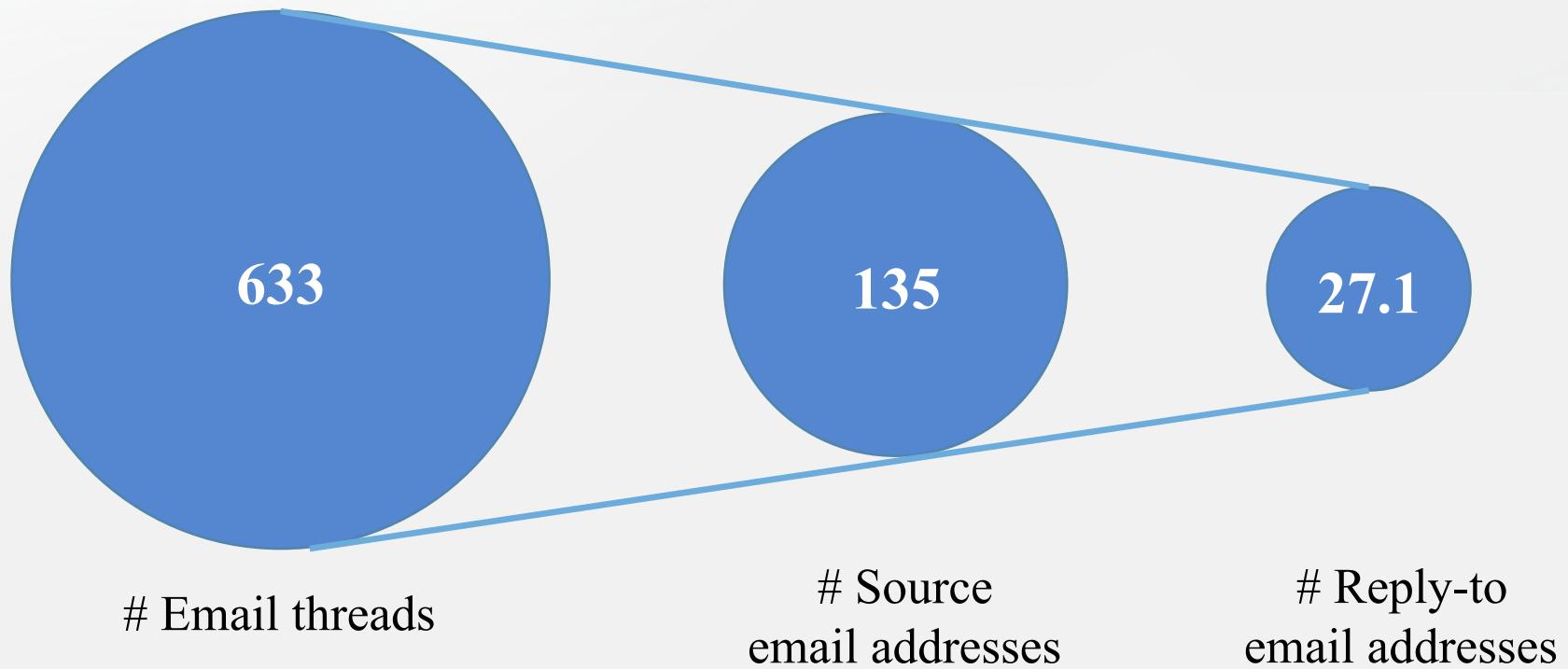
Top 10 IP addresses by  
the number of times observed

# Scammer IP address analysis



# Top 10 groups

- Email account reuse
  - 97% of emails received from top 10 groups have **different source and reply-to addresses**



# Scammer email accounts analysis

Email Provider	Percentage	Relative market share estimation	IMAP/SMTP	Hide sender IP?	Price for 1000 PVAs
Gmail	<b>65.0%</b>	<b>25.0%</b>	<b>Yes</b>	<b>Yes</b>	<b>\$90</b>
Microsoft	10.0%	20.3%	No (POP3/SMTP)	Yes	\$5
AOL	4.9%	11.9%	Yes	No	\$50
Yahoo	3.5%	42.8%	Yes (\$20)	No	\$15
Others	16.6%	-	-	-	-

\* PVA (Phone Verified Accounts)

# Level of automation

Stage	Signs of automation	Signs of manual labor
<b>Reading in Craigslist ads</b>	Short inter-arrival time of first response, Broken scripts in email subject, Duplicate/template email contents	Received emails peak during work hours
<b>First scam response</b>		
<b>Second and later scam responses</b>	Short inter-arrival time of second responses, Duplicate/template responses	Scammers' curse emails, Received emails peak during work hours
<b>Fake payment notification</b>	Duplicate/template responses	Wrong email address/name in the notification

- **Conclusion**
  - Both first and second responses are **partially automated**
  - Scammers may need to **manually run or attend to automated tools**